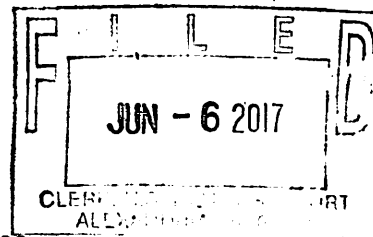


UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia



In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

THE PREMISES LOCATED AT
3234 Tranquility Lane
Herndon, Virginia 20171

Case No. 1:17-SW-306

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252 and 2252A	Received and possessed child pornography.

The application is based on these facts:

See attached Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA
Nathaniel Smith, III

Tonya Sturgill Griffith
Applicant's signature
Special Agent Tonya Sturgill Griffith
Printed name and title

Sworn to before me and signed in my presence.

Date: June 6, 2017

City and state: Alexandria, Virginia

/s/ JFA
John F. Anderson
United States Magistrate Judge
Judge's signature
Honorable John F. Anderson
Printed name and title

ATTACHMENT A
DESCRIPTION OF THE PREMISES TO BE SEARCHED

The Subject Premises, 3234 Tranquility Lane, Herndon, Virginia 20171 is a two-story single-family residence with light colored siding and a red front door with a clear storm door. To the left of the front door is a light colored plaque with "3234" in dark colored numerals.

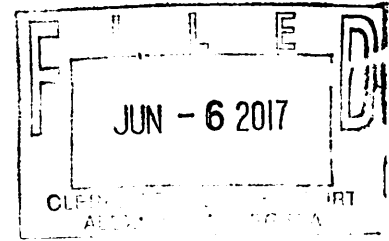
ATTACHMENT B
ITEMS TO BE SEIZED

The following items to be seized constitute contraband, fruits, instrumentalities, and evidence of crimes, to wit: violations of Title 18, United States Code, Sections 2252(a) and 2252A(a) relating to the distribution, receipt and possession of visual depictions of minors engaging in sexually explicit conduct and child pornography:

- a. Child pornography;
- b. Child erotica;
- c. Visual depictions of minors engaged in sexually explicit conduct;
- d. Information, correspondence, records, documents or other materials constituting evidence of or pertaining to items "a" through "c" above (namely child pornography, child erotica, and visual depictions of minors engaged in sexually explicit conduct), or constituting evidence of or pertaining to the possession, receipt, distribution, or transmission through interstate or foreign commerce of items "a" and "c" above, or constituting evidence of or pertaining to an interest in child pornography or sexual activity with children, including:
 - i. Correspondence or communications, such as electronic mail, chat logs, and electronic messages;
 - ii. Internet usage records, user names, logins, passwords, e-mail addresses and identities assumed for the purposes of communication on the Internet, billing, account, and subscriber records, chat room logs, chat records, membership in online groups, clubs or services, connections to online or remote computer storage, and electronic files;
 - iii. Diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the computer and internet websites;
 - iv. Shared images, "friends lists," and "thumbnails"; and
 - v. Financial records, including credit card information.
- e. The items listed in "a" through "d" above may be seized in whatever form, visual or aural, and by any means by which they may have been created, stored, or found, including:

- i. Any computer, computer hardware (including input/output peripheral devices), computer software, router, computer-related documentation, related peripherals, and digital cameras, including:
 - * tapes, tape systems, and tape drives, cassettes, cartridges, streaming tapes, disks, disk drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks;
 - * hard drive and other computer related operation equipment;
 - * monitors, printers, modems, scanners;
 - * hardware and software manuals, passwords, data security devices;
 - * related documentation;
 - ii. Handmade form, including writings, drawings, paintings;
 - iii. Photographic form, including microfilm, microfiche, prints, slides, motion picture, films, videos and photocopies;
 - iv. Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including but not limited to JPG, GIF, TIF, AVI, MPG, and MPEG);
 - v. Mechanical form, including books, magazines, printing, and typing;
 - vi. Electrical, electronic or magnetic form, including
 - * tape recordings, cassettes, compact disks, backup tapes;
 - * electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMS, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multimedia Cards (MMCs), memory sticks, flash memory devices, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks;
 - * digital data files;
 - * printouts or readouts from any magnetic, electrical or electronic storage device; and
 - vii. Originals, photocopies, other copies and negatives.
- f. Records or documents evidencing occupancy or ownership of the Subject Premises, including utility and telephone bills, mail envelopes, or addressed correspondence.
- g. Records or documents evidencing ownership or use of computer equipment found in the Subject Premises, including sales receipts, bills for Internet access, and handwritten notes.

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA



IN RE SEARCH OF:

THE PREMISES LOCATED AT
3234 Tranquility Lane
Herndon, Virginia 20171

Criminal No. 1:17-SW-306

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Tonya Sturgill Griffith, a Special Agent with the Federal Bureau of Investigation (FBI), Washington Field Division, Washington, D.C., being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent of the FBI since February 2002 and am currently assigned to the Washington Field Office, Northern Virginia Resident Agency, Crimes Against Children Task Force. Since joining the FBI, I have investigated violations of federal law involving organized crime, drug trafficking, extra-territorial crime, and terrorism, and I currently investigate federal violations concerning child pornography and the sexual exploitation of children. I have gained experience through training and work related to conducting these types of investigations.

2. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States.

3. This affidavit is made in support of an application for a warrant to:

a. search the entire premises located at 3234 Tranquility Lane, Herndon, VA, 20171 (the "Subject Premises")—which is more particularly described in Attachment A—

inclusive of the computers, computer hardware, computer software, and computer-related documentation found there; and

b. seize the items specified in Attachment B, which constitute instrumentalities, fruits, contraband, and evidence of violations of Title 18, United States Code, Sections 2252 and 2252A.

4. I am familiar with the information contained in this Affidavit based upon the investigation I have conducted, which includes conversations with law enforcement officers and others and review of reports and database records.

5. Because I submit this Affidavit for the limited purpose of securing a search warrant, I have not included each and every fact known to me or the government. I have included only those facts necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Sections 2252 and 2252A is located at the Subject Premises.

CHARACTERISTICS OF CHILD PORNOGRAPHERS

6. My knowledge of preferential sex offenders and their characteristics is based on my experience as an FBI agent, on the training I have received at FBI in-service schools, and training conferences focused on crimes against children. Based upon such training and experience, as well as upon information provided to me by other law enforcement officers, I am aware of the following general characteristics, which may be exhibited in varying combinations:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses (such as in person, in photographs, or other visual media), or from literature describing

such activity. Due to the accessibility and availability of child pornography on the Internet, in my recent experience, instead of maintaining collections, some offenders engage in a pattern of viewing or downloading child pornography online and then deleting the material.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. They may also use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the individual to view the collection, which is valued highly.

d. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

e. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior

has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

f. Individuals whose sexual interest in children or images of children has led them to purchase access to paid websites or other commercial sources of child pornography frequently maintain the financial records of those transactions at their residences.

COMPUTERS AND CHILD PORNOGRAPHY

7. Based upon my training and experience as well as my discussions with others involved in child pornography investigations, computers and computer technology have revolutionized the way in which child pornography is produced, distributed, received and possessed:

a. Child pornographers can transfer photographs to a computer directly from a digital camera or from a regular camera by using a scanner. A computer's electronic storage media (commonly referred to as the hard drive) can store tens of thousands of images at a very high resolution. In addition, magnetic storage located in host computers make it possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image in another country. Once done, there is no readily apparent evidence at the "scene of the crime." Only careful laboratory examination of electronic storage devices can recreate the evidence trail.

b. A modem allows a computer to connect to another through a telephone, cable, or wireless connection to allow contact with millions of computers around the world. And the Internet and World Wide Web provide child pornographers several relatively secure and anonymous ways to obtain, view and trade child pornography. Users can find individuals with similar interests or child pornography websites. Distributors can use membership and

subscription-based websites to conduct business.

c. Collectors and distributors of child pornography can set up an account with a remote computing service that provides e-mail services and electronic file storage.

Evidence of such online storage of child pornography may be found on the user's computer.

d. Information can be saved or stored intentionally on a computer. For example, a person may save an e-mail as a file or may save a favorite website in a "bookmark" type file. Information can also be retained unintentionally. For example, traces of an electronic communication path may be stored automatically in temporary files or Internet Service Provider client software. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Internet distributors and recipients of child pornography may be identified by examining the recipient's computer, including the Internet history and cache to look for "footprints" of the websites and images accessed by the recipient. A forensic examiner often also can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded.

e. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive or viewed via the Internet. Even when such files have been deleted, they can be recovered by forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside for long periods of time in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space (free space or slack space). In addition, a computer's operating system may also

keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

SEARCH AND SEIZURE OF COMPUTER SYSTEMS

8. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including, hard disk drives, floppy disks, compact disks, digital video disks, magnetic tapes, memory chips, memory cards and thumb drives.

9. I also know that it is not always possible to search computer equipment and storage devices during the search of the premises for data for a number of reasons. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. The volume of computer hardware and software in use today renders it difficult to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system being searched.

10. Searching computer systems requires the use of procedures designed to maintain the integrity of the evidence and recover “hidden,” erased, compressed, encrypted, or password-

protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if procedures are not followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is needed to conduct a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

11. The volume of data stored on many computer systems and storage devices will typically be too large to practically search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text, one high-resolution photograph, twenty or more low resolution images, or a couple of short movie clips. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text, one thousand high resolution photographs, or twenty to thirty minutes of high-resolution video. Storage devices capable of storing one hundred gigabytes of data are now commonplace in desktop and laptop computers. Consequently, each non-networked computer can easily contain the equivalent of 50 million pages of data—which, if printed out, would completely fill a 10' x 25' x 12' room to the ceiling—or twenty feature-length high-definition movies.

12. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into viewable form. In addition, computer users can conceal data within another

seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

13. To fully retrieve data from a computer system, the forensic analyst needs all magnetic storage devices, the central processing unit of the computer, and any peripherals or computer equipment attached to the computer, such as printers, modems, routers, external hard drives, and monitors. The analyst also needs all system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media). Peripheral devices allow users to enter or retrieve data from the storage devices and vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In cases like the instant one where the evidence consists partly of image files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce.

PROBABLE CAUSE TO SEARCH THE SUBJECT PREMISES

14. On or about September 8, 2016, the Jackson Office of the FBI executed a search warrant in Mississippi based on information that someone at the residence was distributing and/or receiving child pornography via a peer-to-peer file sharing program. During the on-scene preview of the digital media, it was discovered one of the residents, Phillip Spear, had recorded

himself engaging in a sex act with minors who were in his care and at least one infant.¹

15. A forensic review was conducted by the Jackson Office of the FBI on the digital media seized pursuant to the search warrant. The forensic review recovered an ongoing online dialog between Spear and another individual using the online name “Teddy Ryan” spanning from 2009 through 2015, however based on the conversations, it appears the men had known each other prior to that time.

16. The conversations between 2009 and 2012 occur on Yahoo! Instant Messenger with Ryan utilizing the screen name “coold0101.” During this time, the men discuss Spear attempting to or engaging in sex acts with the three minors (hereinafter referred to as M1, M2 or M3) in his care. On one occasion in March 2012, Spear leaves his webcam on to allow Ryan to watch him engage in a sex act with M2 who was approximately 14 years old. The men also discuss having Ryan pay the three minors in Spear’s care to send sexually explicit images of themselves and eventually travel to Spear’s home to engage in sexual activity with the minors.

17. During 2012, the men also discuss images of child pornography. Both men state they are obtaining images by accessing an email account belonging to a woman Ryan communicates with. In addition to the images, Ryan states the woman provides “live online” shows with members of her family who are minors. Spear also tells Ryan of a peer-to-peer file sharing site which he has used to download images of child pornography.

18. In early 2013, the men begin communicating via Skype with Ryan utilizing the screen name “Cooldskypetransfer”. On or about January 13, 2013, Spear and Ryan exchange multiple files after discussing “good pics of the little ones”, which could not be forensically

¹ The subject of the referenced investigation has subsequently pleaded guilty to a six count indictment, including charges of Production, Transportation, Distribution and Possession of Child Pornography. Southern District of Mississippi Criminal Case #1:17-cr-00017-LG-RHW.

recovered. Spear tells Ryan “don’t forget to pay (M1, now 16 years old)... she made the last one after ur little talk with her on FB... Do that again if u would!”

19. On or about July 27, 2013, Spear and Ryan exchange a number of files which could not be recovered, however, Spear states “little girl remind me of (M2) when i first met them” and “that’s so nice... love those girls”. Spear also states he almost has M2 (now 16 years old) “talked into doing some nauty photos” for Ryan and M2 asked how much Ryan would pay her. One video sent by Spear to Ryan was recovered. The video depicts M3 at approximately 14-15 years of age, performing oral sex on an adult male.

20. On or about August 24, 2014, Spear sends Ryan several unrecovered video segments and states they are of M3 (now 16 years old) “last video adventure.” In response, Ryan states “WOW her tits got lovely”. Spear then sends Ryan a video stating “oh and I fucked the hell out of M3 for ya in that vid...tried to hurt that pussy”. Later in the conversation Spear suggests sharing a Yahoo! Email account which would allow the men to share videos via draft emails. Ryan then creates the account tryan0101@yahoo.com and provides Spear with the password. Spear states the account only allows 25MB at a time and tells Ryan once he has downloaded the content, Spear will add more.

21. On or about August 29, 2014, Spear suggests creating a Dropbox account as it would allow larger files than the email account. Ryan then creates a Dropbox account utilizing the email tryan0101@gmail.com and provides Spear with the password.

22. On or about September 4, 2014, Spear messages Ryan “i think i can make some more video for ya tomorrow with either M3 (now 16 years old) or M1 (now 18 years old)...which one u like?” Spear later states it will be M3 to which Ryan replies “nice” “so yummy”.

23. On or about October 16, 2014, Ryan tells Spear he “did a little rubbing recently” and explains his girlfriend was watching a four month old and while the girlfriend was asleep he “had his way” with the infant.

24. On or about January 23, 2015, Ryan tells Spear he is going to have a “litl snack” referencing a sexual act with a seven month old.

25. On or about April 18, 2015, Spear and Ryan have a discussion about how the two had met and Spear calls Ryan “Todd”.

26. From this time until the last recovered contact in August 2015, Spear and Ryan discuss the possibility of Ryan traveling to see Spear and engage in sexual acts. By this time, only one of the three individuals in Spear’s care is still a minor.

27. On or about February 6, 2017, pursuant to an administrative subpoena, Google provided tryan0101@gmail.com (the account associated with the Dropbox account) was created on August 29, 2014 utilizing IP address 96.255.132.84, which was registered to Verizon.

28. On or about February 21, 2017, pursuant to legal process, Verizon reported at the time the Google email was created IP address 96.255.132.84 was assigned to Todd McAlister, 3234 Tranquility Lane, Herndon, VA 20171.

29. A Facebook page in the name of Teddy Ryan was located and pursuant to legal process, Facebook provided coold0101@yahoo.com was associated with the Facebook account. In addition, IP address 96.255.132.84 was utilized to access the Facebook account during the time frame it was assigned to McAlister.

30. A Facebook page in the name of Todd McAlister was also located and it contained the same profile picture that was found on the Teddy Ryan Facebook page.

31. Open source data base checks conducted in May 2017 indicated McAlister was


still associated with the Subject Premises.

CONCLUSION


32. Based on the above information, there is probable cause to believe that (1) an individual residing at the Subject Premises used a computer connected to the Internet from the Subject Premises to violate Title 18, United States Code, Sections 2252 and 2252A, which make it a federal crime for any person to knowingly receive, distribute or possess child pornography; and (2) the fruits, evidence, contraband and instrumentalities of these offenses, described in Attachment B are located at the Subject Premises.

33. Based upon the foregoing, I respectfully request that this Court issue a search warrant for the Subject Premises, more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B.

Respectfully submitted,


Tonya Sturgill Griffith
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
this 6th day of June 2017.

 /s/ 
John F. Anderson
United States Magistrate Judge
The Honorable John F. Anderson
United States Magistrate Judge

ATTACHMENT A
DESCRIPTION OF THE PREMISES TO BE SEARCHED

The Subject Premises, 3234 Tranquility Lane, Herndon, Virginia 20171 is a two-story single-family residence with light colored siding and a red front door with a clear storm door. To the left of the front door is a light colored plaque with "3234" in dark colored numerals.

ATTACHMENT B
ITEMS TO BE SEIZED

The following items to be seized constitute contraband, fruits, instrumentalities, and evidence of crimes, to wit: violations of Title 18, United States Code, Sections 2252(a) and 2252A(a) relating to the distribution, receipt and possession of visual depictions of minors engaging in sexually explicit conduct and child pornography:

- a. Child pornography;
- b. Child erotica;
- c. Visual depictions of minors engaged in sexually explicit conduct;
- d. Information, correspondence, records, documents or other materials constituting evidence of or pertaining to items “a” through “c” above (namely child pornography, child erotica, and visual depictions of minors engaged in sexually explicit conduct), or constituting evidence of or pertaining to the possession, receipt, distribution, or transmission through interstate or foreign commerce of items “a” and “c” above, or constituting evidence of or pertaining to an interest in child pornography or sexual activity with children, including:
 - i. Correspondence or communications, such as electronic mail, chat logs, and electronic messages;
 - ii. Internet usage records, user names, logins, passwords, e-mail addresses and identities assumed for the purposes of communication on the Internet, billing, account, and subscriber records, chat room logs, chat records, membership in online groups, clubs or services, connections to online or remote computer storage, and electronic files;
 - iii. Diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the computer and internet websites;
 - iv. Shared images, “friends lists,” and “thumbnails”; and
 - v. Financial records, including credit card information.
- e. The items listed in “a” through “d” above may be seized in whatever form, visual or aural, and by any means by which they may have been created, stored, or found, including:

- i. Any computer, computer hardware (including input/output peripheral devices), computer software, router, computer-related documentation, related peripherals, and digital cameras, including:
 - * tapes, tape systems, and tape drives, cassettes, cartridges, streaming tapes, disks, disk drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks;
 - * hard drive and other computer related operation equipment;
 - * monitors, printers, modems, scanners;
 - * hardware and software manuals, passwords, data security devices;
 - * related documentation;
 - ii. Handmade form, including writings, drawings, paintings;
 - iii. Photographic form, including microfilm, microfiche, prints, slides, motion picture, films, videos and photocopies;
 - iv. Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including but not limited to JPG, GIF, TIF, AVI, MPG, and MPEG);
 - v. Mechanical form, including books, magazines, printing, and typing;
 - vi. Electrical, electronic or magnetic form, including
 - * tape recordings, cassettes, compact disks, backup tapes;
 - * electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMS, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multimedia Cards (MMCs), memory sticks, flash memory devices, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks;
 - * digital data files;
 - * printouts or readouts from any magnetic, electrical or electronic storage device; and
 - vii. Originals, photocopies, other copies and negatives.
- f. Records or documents evidencing occupancy or ownership of the Subject Premises, including utility and telephone bills, mail envelopes, or addressed correspondence.
- g. Records or documents evidencing ownership or use of computer equipment found in the Subject Premises, including sales receipts, bills for Internet access, and handwritten notes.